JC07 Rec'd PCT/PTO 16 APR 2001

FORM PTO-1390 (Modified) (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: **112740-195**

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR): **09/807690**

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/DE99/02572	**17 August 1999**	**14 October 1998**

TITLE OF INVENTION

APPARATUS AND METHOD FOR THE BIOMETRIC IDENTIFICATION OF A PERSON

APPLICANT(S) FOR DO/EO/US

Bernhard Raaf et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ A copy of the International Search Report (PCT/ISA/210).
8. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
9. ☒ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☒ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

Submission of Drawings Figures 1-2 on one sheet

JC03 Rec'd PCT/PTO 16 APR 2001

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/807690	PCT/DE99/02572	112740-195

21. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☐	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO	**$1,000.00**
☒	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but Internation Search Report prepared by the EPO or JPO	**$860.00**
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	**$710.00**
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4)	**$690.00**
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4)	**$100.00**

ENTER APPROPRIATE BASIC FEE AMOUNT =	**$860.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	6 - 20 =	0	x $18.00	**$0.00**	
Independent claims	2 - 3 =	0	x $80.00	**$0.00**	
Multiple Dependent Claims **(check if applicable)**.			☐	**$0.00**	
TOTAL OF ABOVE CALCULATIONS			=	**$860.00**	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable)**.			☐	**$0.00**	
SUBTOTAL			=	**$860.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).			+	**$0.00**	
TOTAL NATIONAL FEE			=	**$860.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			☐	**$0.00**	
TOTAL FEES ENCLOSED			=	**$860.00**	
				Amount to be: refunded	$
				charged	$

☒ A check in the amount of **$860.00** to cover the above fees is enclosed.

☐ Please charge my Deposit Account No. in the amount of to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **02-1818** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

William E. Vaughan
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, IL 60690-1135

SIGNATURE

William E. Vaughan
NAME

39,056
REGISTRATION NUMBER

April 16, 2001
DATE

BOX PCT

IN THE UNITED STATES ELECTED/DESIGNATED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY-CHAPTER II

APPLICANTS: Bernhard Raaf et al. DOCKET NO: 112740-195

SERIAL NO: GROUP ART UNIT:

EXAMINER:

INTERNATIONAL APPLICATION NO: PCT/DE99/02572

INTERNATIONAL FILING DATE: 17 August 1999

INVENTION: APPARATUS AND METHOD FOR THE BIOMETRIC IDENTIFICATION OF A PERSON

Assistant Commissioner for Patents,
Washington, D.C. 20231

SUBMISSION OF DRAWINGS

Applicants herewith submit one sheet (Figs. 1-2) of drawings for the above-referenced PCT application.

Respectfully submitted,

(Reg. No. 39,056)

William E. Vaughan
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690-1135
(312) 807-4292
Attorneys for Applicants

FIG 1

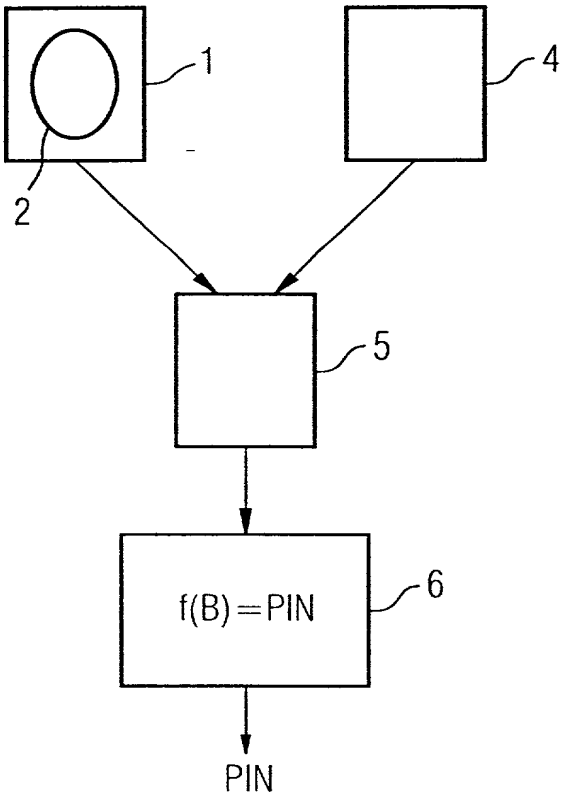
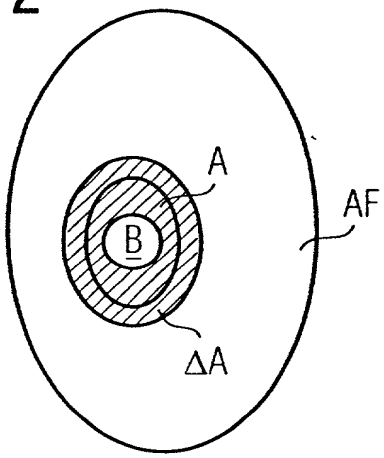


FIG 2



BOX PCT

IN THE UNITED STATES ELECTED/DESIGNATED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY-CHAPTER II

PRELIMINARY AMENDMENT

APPLICANTS:	Bernhard Raaf et al.	DOCKET NO: 112740-195
SERIAL NO:		GROUP ART UNIT:
		EXAMINER:
INTERNATIONAL APPLICATION NO:		PCT/DE99/02572
INTERNATIONAL FILING DATE:		17 August 1999
INVENTION:	APPARATUS AND METHOD FOR THE BIOMETRIC IDENTIFICATION OF A PERSON	

Assistant Commissioner for Patents,
Washington, D.C. 20231

Sir:

Please amend the above-identified International Application before entry into the National stage before the U.S. Patent and Trademark Office under 35 U.S.C. §371 as follows:

In the Specification:

Please replace the Specification of the present application, including the Abstract, with the following Substitute Specification:

SPECIFICATION

TITLE

APPARATUS AND METHOD FOR THE BIOMETRIC IDENTIFICATION OF A PERSON

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to an apparatus and to a method for the biometric identification of a person, having an authentication area containing

biometric features. Such apparatuses and methods are used, for example, in electronic appliances where a user needs to authenticate oneself before using the appliance. Examples of such electronic appliances are telecommunication appliances, such as mobile telephones and computers.

Description of the Prior Art

In mobile telephones, for example, it is usual to use a so-called personal identification number (PIN) as access authorization. In this context, in order to be able to make a telephone call, the user needs to enter a particular PIN which is known only to him. The mobile telephone checks this PIN and, if the check is positive, enables the mobile telephone for the purpose of making calls.

In addition, more general identification codes, like PINs, are used in computers in order to control access to particular data or services of the computer or of a communication network to which the computer is connected.

Usually, the authentication information is entered using a keypad associated with the apparatus and is then checked. In this way, the authorization of the user making the entry is established by the mobile telephone, the computer or the communication network.

In mobile telephones based on the GSM standard, this is done by virtue of a data processing device on the appliance's 'SIM' card checking whether the entered PIN matches the information stored on the SIM card. If this is the case, the SIM card enables the telephone for use. According to the GSM standard, a particularly high level of security is obtained for the telephone customer by virtue of the fact that the PIN must not be stored in the mobile telephone itself, but rather is stored on the SIM card in encrypted form only.

In addition, biometric identification methods have recently been developed in which biological or biometric features of a user are used for authentication purposes. By way of example, the fingerprint of a user is used as unique identification of this user. Such biometric identification is a complex but convenient, and often very secure, method of ensuring that a particular person is

associated with and can access a service, an object or a place. In this context, the advantages of biometric identification over the PIN are that it cannot be forgotten, and that the biometric features can be copied only with very great difficulty, or cannot be copied at all. Whereas the PIN is pure software, biometric features always have a more or less unique association with the hardware; i.e., with the body of the authorized user. Since the PIN entails the entry of digits or text, which usually requires a series of keystrokes, this always results in convenience being diminished and, hence, sometimes in the security measures being bypassed. For example, with some mobile radio services, the user is able to turn off the PIN completely, at his/her own risk. Mobile radio services do not require acknowledgement of each individual telephone call via the PIN. As such, once it has been turned on, a mobile telephone can be used by any third party and, hence, also by unauthorized persons at the cost of the owner of the mobile telephone. Modern mobile telephones are increasingly trying to restrict the entry of digits for telephone numbers to emergencies. Attempts are even being made to manage with mobile telephones with no keypad at all for some applications. In this case, distinctive biometric identification, if it is possible with little effort, is very advantageous.

In current mobile telephones, however, the problem arises that they require the PIN to be stored on the SIM card in order to conform to the GSM standard, as explained above. In accordance with the GSM standard, this PIN must not be additionally stored in the mobile telephone itself. The problem which this poses is that the PIN cannot be completely replaced by biometric identification without changing the GSM standard.

For this reason, a method has been proposed in which a unique identification number can be derived from biometric features. This unique identification number can, accordingly, be used as a PIN and, by way of example, can be forwarded to the SIM card of a mobile telephone. It is evident that, in this

case, the PIN is not stored in the mobile telephone itself, but rather is merely calculated by the latter from detected biometric features.

If an authentication area of a person, such as the fingerprint of the person, is used, this authentication area contains biometric features which uniquely identify the person. In this context, the total authentication area, i.e. the fingerprint area, which can be used to identify the user is usually larger than the identification area of a sensor detecting the biometric features of the person's authentication area. This means that the sensor uses only part of the person's authentication area to derive the unique identification number. Accordingly, variations in position, for example of the fingerprint area, on the identification area of the sensor can result in different identification numbers. Such different identification numbers for a user cannot be used as a PIN and make unique identification of the user more difficult.

It is an object of the present invention, therefore, to provide an apparatus and a method for the biometric identification of a person, who has an authentication area containing biometric features, in which a unique identification number can be derived irrespective of variations in the positioning of the part of the person's authentication area which is situated on the identification area of the sensor.

SUMMARY OF THE INVENTION

Accordingly, the present invention provides an apparatus for the biometric identification of a person, who has an authentication area containing biometric features, including a sensor having an identification area for detecting the biometric features of the part of the person's authentication area which is situated on the identification area, a comparison device for comparing the detected biometric features of the first area with the biometric features, stored in a memory, of a part of the authentication area of an authorized person or of a number of authorized persons and for determining the relative position of the biometric features detected by the sensor within the part of the authentication

area, and a computation device for calculating an identification code, which identifies the person detected by the sensor, from the detected biometric features which are not stored in the memory 4 on the basis of the relative position of the biometric features which are stored in the memory (4) within the stored authentication area.

An advantage of the apparatus according to the present invention is that the identification area of the sensor is split into two regions, with one region being used for position determination within the authentication area while the second region is used to generate a unique identification number, the biometric features of this region not being stored in the apparatus. This ensures that, even if different portions of the user's authentication area are in contact with the identification area of the sensor, it is always possible to calculate a unique identification code which characterizes the user.

In one embodiment of the present invention, the sensor detects the fingerprint of a person, the person's authentication area including the possible fingerprint areas of a finger of this person which are not used to calculate the identification code.

An advantage of the use of a fingerprint sensor is that the user can firstly place a finger on the sensor without any particular trouble and, secondly, the biometric features of the fingerprint area permit particularly reliable identification of the user.

In addition, the present invention provides an appropriate method for the biometric identification of a person via an authentication area containing biometric features.

The fact that, in one embodiment of the method of the present invention, the identification area is subdivided such that the region used for the position determination within the authentication area completely surrounds the area used to calculate the identification code ensures that the second, enclosed region

always contains sufficient biometric features to calculate a unique identification code.

Additional features and advantages of the present invention are described in, and will be apparent from, the Detailed Description of the Preferred Embodiments and the Drawings.

DESCRIPTION OF THE DRAWINGS

Figure 1 shows a schematic illustrative embodiment of the apparatus of the present invention; and

Figure 2 shows one possible position of that region of a person's authentication area which is detected by the identification area of the sensor.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the illustrative embodiment explained here, the present invention contemplates an apparatus and a method which uses a person's fingerprint to identify such person. Hence, the person's authentication area is part of the total fingerprint area of a finger of this person. In addition, the biometric features of the fingerprint area are the line ends and bifurcations of the corresponding fingerprint.

Figure 1 shows, schematically, an illustrative embodiment of the apparatus according to the present invention. The sensor 1 is used to detect part of the total fingerprint area of a finger of the person who is to be identified. To this end, the sensor 1 has an identification area 2 onto which the user places the finger. Since the identification area 2 is smaller than the total fingerprint area of a finger, the identification area 2 is used to detect a particular portion of the fingerprint. The identification area 2 is used to detect the biometric features of the part of the total fingerprint area which is in contact. The information detected by the sensor 1 is supplied to a comparison device 5.

When the apparatus is initialized, i.e. before a person is first identified, the part of the total authentication area of the authorized person(s) which is required to determine the position of the detected biometric features is stored in a memory 4. By way of example, a region of the area $A - B + \Delta A$ may be stored, where ΔA

forms a ring having a particular tolerance width around A. In the illustrative embodiment described in this case, this means that the fingerprint area of a finger of the authorized person(s) which is used to determine the identification code is not stored in the memory 4.

The comparison device 5, which is connected both to the sensor 1 and to the memory 4, compares the detected biometric features with the biometric features stored in the memory 4. A match between the biometric features of a region A, for example, and a geometric region within the authentication area stored in the memory 4 gives the relative position of the detected region A within the authentication area. This comparison gives the information about which part of the fingerprint has been placed onto the identification area 2 of the sensor 1. Hence, the outer region A is used for centering, while the central region B surrounded by the region A is used later to generate the identification code or the PIN. The regions A, B are thus advantageously chosen such that the outer region A forms a ring, containing biometric features, which completely surrounds the central region B. However, in another embodiment of the present invention, the biometric features may also be split into two regions differently. By way of example, the right-hand and left-hand halves or the top and bottom halves could be chosen as the subdivision. In addition, the branches and the line ends of the fingerprint could be used as the subdivision.

For the purposes of centering, it is not absolutely necessary for the outer region A to be complete; i.e., to contain biometric features throughout. If there are variations in the contact of the finger on the identification area 2, it is possible that no biometric features are detected at the extreme edge of the outer region A. If, however, biometric features are detected in a closed ring, surrounding the central region B, of the outer region A and have their position determined via comparison with the authentication area stored in the memory 4, then at least the central region B is available in its entirety and in the correct position. In addition, in a learning phase when the apparatus is initialized, it is possible for an algorithm to

decide what belongs to the central region B and what belongs to the outer region A.

The comparison device 5 supplies the result of the position determination for the part of the total fingerprint area which is detected by the sensor 1 to a computation device 6. The computation device 6 calculates from the biometric features of the central region B, whose relative position is determined from the position of the region A, an identification code which uniquely identifies the person detected by the sensor 1. This identification code may be a PIN, for example, which is supplied to the SIM card of the mobile telephone.

Hence, neither the PIN nor the biometric features from which the PIN is calculated are stored in the inventive apparatus itself. The only thing stored in the memory 4 of the apparatus is part of the authentication area containing biometric features. The sensor 1 is used to detect biometric features of a person, and the computation device 6 is used to convert them into a PIN which then can be output. In addition, the person's PIN or identification code can be derived even if, for different identification operations, a different part of the authentication area of the person has been placed on the identification area 2 of the sensor 1 in each case.

Figure 2 is intended to be used to illustrate the ratio of the person's total authentication area to the part of the authentication area which is stored in the memory 4 and to the part of this authentication area which is detected via the identification area of the sensor 1. For the purposes of illustration, the identification of a person via the biometric features of a fingerprint is again used as an example. In this case, the authentication area AF is the fingerprint area of a finger of the person. The total range of this authentication area contains biometric features which uniquely identify a person. Of these, the part which is shown shaded is stored in the memory 4. This part is given by the area of the region A less the area of the region B plus a tolerance region ΔA for the region A.

When the person places his finger to be used for identification onto the identification area 2 of the sensor 1, the sensor 1 detects a particular part of the total fingerprint area AF. This is illustrated in Figure 2 via the ellipse surrounding the area A within the region AF. Depending on the position of the finger on the identification area 2 of the sensor 1, this ellipse moves within the region AF stored in the memory 4.

The part of the authentication area which is detected via the sensor 1 is subdivided into two regions A and B. The biometric features of the region A now can be compared with biometric features of the area AF stored in the memory 4 which have a geometrically identical arrangement. If a match has been determined, the position of the region A within the authentication area AF is obtained unambiguously, and hence so too is the position of the second region B, since the latter region is in a particular, in this case geometrical, relationship with respect to the region A. This information and the biometric features of the second region B then can be used to calculate the identification code or the PIN.

Although the present invention has been described with reference to specific embodiments, those of skill in the art will recognize that changes may be made thereto without departing from the spirit and scope of the invention as set forth in the hereafter appended claims.

ABSTRACT OF THE DISCLOSURE

An apparatus and method for the biometric identification of a person, who has an authentication area containing biometric features, the apparatus including a sensor having an identification area for detecting the biometric features of the part of the person's authentication area which is situated on the identification area, a comparison device for comparing the detected biometric features with the biometric features, stored in a memory, of a part of the authentication area of an authorized person or of a number of authorized persons in order to determine the relative position of the biometric features detected by the sensor within the part of the authentication area, and a computation device for calculating an identification

code, which identifies the person detected by the sensor, from the detected biometric features which are not stored in the memory on the basis of the relative position of the biometric features which are stored in the memory within the stored authentication area .

In the claims:

On page 10, cancel line 1, and substitute the following left-hand justified heading therefor:

We Claim as Our Invention:

Please cancel claims 1-6, without prejudice, and substitute the following claims therefor:

7. An apparatus for biometric identification of a person, who has an authentication area containing biometric features, comprising:

a sensor having an identification area for detecting biometric features of a part of the authentication area which is situated on the identification area,

a comparison device for comparing the detected biometric features with biometric features, stored in a memory, of a part of the authentication area of at least one authorized person to determine a relative position of the detected biometric features of a first detected region within the part of the authentication area; and

a computation device for calculating an identification code, which identifies the person detected by the sensor, from the detected biometric features which are not stored in the memory based on the relative position of the biometric features which are stored in the memory within the stored authentication area.

8. An apparatus for biometric identification of a person as claimed in claim 1, wherein the sensor detects a fingerprint, and the authentication area includes those parts of the possible fingerprint area of a finger which are not used to calculate the identification code.

9. A method for biometric identification of a person, who has an authentication area containing biometric features, the method comprising the steps of:

storing biometric features of a part of the authentication area of at least one authorized person;

detecting biometric features of the part of the person's authentication area which is situated on the identification area;

comparing the detected biometric features with the stored biometric features of the authentication area to determine a relative position of the detected biometric features within the stored part of the authentication area; and

calculating an identification code which identifies the person detected by the sensor from the detected biometric features which are not stored in the memory based on the relative position of the biometric features which are stored in the memory within the stored authentication area.

10. A method for biometric identification of a person as claimed in claim 3, wherein biometric features of a person's fingerprint are detected, and the authentication area includes those parts of the possible fingerprint areas of a finger of the person which are not used to calculate the identification code.

11. A method for biometric identification of a person as claimed in claim 3, wherein a first region containing biometric features which are stored in the memory completely surrounds a second region containing biometric features which are not stored in the memory.

12. A method for biometric identification of a person as claimed in claim 5, wherein an identification code is calculated only if the detected first region forms a closed ring, surrounding the second region, containing biometric features.

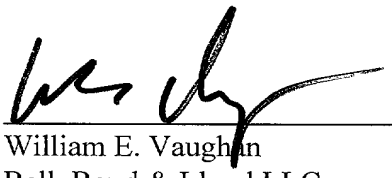
REMARKS

The present amendment makes editorial changes and corrects typographical errors in the specification, which includes the Abstract, in order to conform the specification to the requirements of United States Patent Practice. No new matter is added thereby. Attached hereto is a marked-up version of the changes made to the specification by the present amendment. The attached page is captioned "**Version With Markings To Show Changes Made".**

In addition, the present amendment cancels original claims 1-6 in favor of new claims 7-12. Claims 7-12 have been presented solely because the revisions by red-lining and underlining which would have been necessary in claims 1-6 in order to present those claims in accordance with preferred United States Patent Practice would have been too extensive, and thus would have been too burdensome. The present amendment is intended for clarification purposes only and not for substantial reasons related to patentability pursuant to 35 USC §§103, 102, 103 or 112. Indeed, the cancellation of claims 1-6 does not constitute an intent on the part of the Applicants to surrender any of the subject matter of claims 1-6.

Early consideration on the merits is respectfully requested.

Respectfully submitted,



(Reg. No. 39,056)

William E. Vaughan
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690-1135
(312) 807-4292
Attorneys for Applicants

VERSIONS WITH MARKINGS TO SHOW CHANGES MADE

In The Specification:

The Specification of the present application, including the Abstract, has been amended as follows:

SPECIFICATION

TITLE

APPARATUS AND METHOD FOR THE BIOMETRIC IDENTIFICATION OF A PERSON

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to an apparatus and to a method for the biometric identification of a person~~, who has~~ having an authentication area containing biometric features. Such apparatuses and methods are used, for example, in electronic appliances where a user needs to authenticate ~~himself~~ oneself before using the appliance. Examples of such electronic appliances are telecommunication appliances, such as mobile telephones~~,~~ and computers.

Description of the Prior Art

In mobile telephones, for example, it is usual to use a so-called personal identification number (PIN) as access authorization. In this context, in order to be able to make a telephone call, the user needs to enter a particular PIN which is known only to him. The mobile telephone checks this PIN and, if the check is positive, enables the mobile telephone for the purpose of making calls.

In addition, more general identification codes, like PINs, are used in computers in order to control access to particular data or services of the computer or of a communication network to which the computer is connected.

Usually, the authentication information is entered using a keypad associated with the apparatus and is then checked. In this way, the authorization of the user making the entry is established by the mobile telephone, the computer or the communication network.

In mobile telephones based on the GSM standard, this is done by virtue of a data processing device on the appliance's 'SIM' card checking whether the entered PIN matches the information stored on the SIM card. If this is the case, the SIM card enables the telephone for use. According to the GSM standard, a particularly high level of security is obtained for the telephone customer by virtue of the fact that the PIN must not be stored in the mobile telephone itself, but rather is stored on the SIM card in encrypted form only.

In addition, biometric identification methods have recently been developed in which biological or biometric features of a user are used for authentication purposes. By way of example, the fingerprint of a user is used as unique identification of this user. Such biometric identification is a complex but convenient, and often very secure, method of ensuring that a particular person is associated with and can access a service, an object or a place. In this context, the ~~advantage~~ advantages of biometric identification over the PIN ~~is~~ are that it cannot be forgotten, and that the biometric features can be copied only with very great difficulty, or cannot be copied at all. Whereas the PIN is pure software, biometric features always have a more or less unique association with the hardware~~,~~; i.e., with the body of the authorized user. Since the PIN entails the entry of digits or text, which usually requires a series of keystrokes, this always results in convenience being diminished~~,~~ and, hence, sometimes in the security measures being bypassed. For example, with some mobile radio services, the user is able to turn off the PIN completely, at his/her own risk. Mobile radio services do not require acknowledgement of each individual telephone call ~~by means of~~ via the PIN. ~~This means that,~~ As such, once it has been turned on, a mobile telephone can be used by any third ~~parties~~ party and, hence, also by unauthorized persons at the cost of the owner of the mobile telephone. Modern mobile telephones are increasingly trying to restrict the entry of digits for telephone numbers to emergencies. Attempts are even being made to manage with mobile telephones

with no keypad at all for some applications. In this case, distinctive biometric identification, if it is possible with little effort, is very advantageous.

In current mobile telephones, however, the problem arises that they require the PIN to be stored on the SIM card in order to conform to ~~standard on the basis of~~ the GSM standard, as explained above. In accordance with the GSM standard, this PIN must not be additionally stored in the mobile telephone itself. The problem which this poses is that the PIN cannot be completely replaced by biometric identification without changing the GSM standard.

For this reason, a method has been proposed in which a unique identification number can be derived from biometric features. This unique identification number can, accordingly, be used as a PIN and, by way of example, can be forwarded to the SIM card of a mobile telephone. It is evident that, in this case, the PIN is not stored in the mobile telephone itself, but rather is merely calculated by the latter from detected biometric features.

If an authentication area of a person, such as the fingerprint of the person, is used, this authentication area contains biometric features which uniquely identify the person. In this context, the total authentication area, i.e. the fingerprint area, which can be used to identify the user is usually larger than the identification area of a sensor detecting the biometric features of the person's authentication area. This means that the sensor uses only part of the person's authentication area to derive the unique identification number. Accordingly, variations in position, for example of the fingerprint area, on the identification area of the sensor can result in different identification numbers. Such different identification numbers for a user cannot be used as a PIN and make unique identification of the user more difficult.

It is ~~the~~ an object of the present invention, therefore, to provide an apparatus and a method for the biometric identification of a person, who has an authentication area containing biometric features, in which a unique identification number can be derived irrespective of variations in the positioning of the part of

the person's authentication area which is situated on the identification area of the sensor.

SUMMARY OF THE INVENTION

~~The~~ Accordingly, the present invention provides an apparatus for the biometric identification of a person, who has an authentication area containing biometric features, ~~comprising~~ including a sensor having an identification area for detecting the biometric features of the part of the person's authentication area which is situated on the identification area, a comparison device for comparing the detected biometric features of the first area with the biometric features, stored in a memory, of a part of the authentication area of an authorized person or of a ~~plurality~~ number of authorized persons and for determining the relative position of the biometric features detected by the sensor within the part of the authentication area, and a computation device for calculating an identification code, which identifies the person detected by the sensor, from the detected biometric features which are not stored in the memory 4 on the basis of the relative position of the biometric features which are stored in the memory (4) within the stored authentication area.

An advantage of the apparatus according to the present invention is that the identification area of the sensor is split into two regions, with one region being used for position determination within the authentication area while the second region is used to generate a unique identification number, the biometric features of this region not being stored in the apparatus. This ensures that, even if different portions of the user's authentication area are in contact with the identification area of the sensor, it is always possible to calculate a unique identification code which characterizes the user.

In one embodiment of the present invention, the sensor detects the fingerprint of a person, the person's authentication area ~~comprising~~ including the possible fingerprint areas of a finger of this person which are not used to calculate the identification code.

~~The~~ An advantage of the use of a fingerprint sensor is that the user can firstly place a finger on the sensor without any particular trouble~~,~~ and, secondly, the biometric features of the fingerprint area permit particularly reliable identification of the user.

In addition, the present invention provides an appropriate method for the biometric identification of a person ~~by means of~~ via an authentication area containing biometric features.

The fact that, in one embodiment of the method of the present invention, the identification area is subdivided such that the region used for the position determination within the authentication area completely surrounds the area used to calculate the identification code ensures that the second, enclosed region always contains sufficient biometric features to calculate a unique identification code.

Additional features and advantages of the present invention are described in, and will be apparent from, the Detailed Description of the Preferred Embodiments and the Drawings.

~~Illustrative embodiments of the present invention are now explained with the aid of the drawings.~~

DESCRIPTION OF THE DRAWINGS

Figure 1 shows ~~an~~ a schematic illustrative embodiment of the apparatus of the present invention~~,~~; and

Figure 2 shows one possible position of that region of a person's authentication area which is detected by the identification area of the sensor.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the illustrative embodiment explained here, the present invention ~~is explained using~~ contemplates an apparatus and a method which uses a person's fingerprint to identify ~~this~~ such person. Hence, the person's authentication area is part of the total fingerprint area of a finger of this person. In addition, the

biometric features of the fingerprint area are the line ends and bifurcations of the corresponding fingerprint.

Figure 1 shows, schematically, an illustrative embodiment of the apparatus according to the present invention. The sensor 1 is used to detect part of the total fingerprint area of a finger of the person who is to be identified. To this end, the sensor 1 has an identification area 2 onto which the user places the finger. Since the identification area 2 is smaller than the total fingerprint area of a finger, the identification area 2 is used to detect a particular portion of the fingerprint. The identification area 2 is used to detect the biometric features of the part of the total fingerprint area which is in contact. The information detected by the sensor 1 is supplied to a comparison device 5.

When the apparatus is initialized, i.e. before a person is first identified, the part of the total authentication area of the authorized person(s) which is required to determine the position of the detected biometric features is stored in a memory 4. By way of example, a region of the area $A - B + \Delta A$ may be stored, where ΔA forms a ring having a particular tolerance width around A. In the illustrative embodiment described in this case, this means that the fingerprint area of a finger of the authorized person(s) which is used to determine the identification code is not stored in the memory 4.

The comparison device 5, which is connected both to the sensor 1 and to the memory 4, compares the detected biometric features with the biometric features stored in the memory 4. A match between the biometric features of a region A, for example, and a geometric region within the authentication area stored in the memory 4 gives the relative position of the detected region A within the authentication area. This comparison gives the information about which part of the fingerprint has been placed onto the identification area 2 of the sensor 1. Hence, the outer region A is used for centering, while the central region B surrounded by the region A is used later to generate the identification code or the PIN. The regions A, B are thus advantageously chosen such that the outer region

A forms a ring, containing biometric features, which completely surrounds the central region B. However, in another embodiment of the present invention, the biometric features may also be split into two regions differently. By way of example, the right-hand and left-hand halves or the top and bottom halves could be chosen as the subdivision. In addition, the branches and the line ends of the fingerprint could be used as the subdivision.

For the purposes of centering, it is not absolutely necessary for the outer region A to be complete~~,~~; i.e., to contain biometric features throughout. If there are variations in the contact of the finger on the identification area 2, it is possible that no biometric features are detected at the extreme edge of the outer region A. If, however, biometric features are detected in a closed ring, surrounding the central region B, of the outer region A and have their position determined ~~by means of~~ via comparison with the authentication area stored in the memory 4, then at least the central region B is available in its entirety and in the correct position. In addition, in a learning phase when the apparatus is initialized, it is possible for an algorithm to decide what belongs to the central region B and what belongs to the outer region A.

The comparison device 5 supplies the result of the position determination for the part of the total fingerprint area which is detected by the sensor 1 to a computation device 6. The computation device 6 calculates from the biometric features of the central region B, whose relative position is determined from the position of the region A, an identification code which uniquely identifies the person detected by the sensor 1. This identification code may be a PIN, for example, which is supplied to the SIM card of the mobile telephone.

Hence, neither the PIN nor the biometric features from which the PIN is calculated ~~is~~/are stored in the inventive apparatus itself. The only thing stored in the memory 4 of the apparatus is part of the authentication area containing biometric features. The sensor 1 is used to detect biometric features of a person, and the computation device 6 is used to convert them into a PIN which ~~can~~ then

can be output. In addition, the person's PIN or identification code can be derived even if, for different identification operations, a different part of the authentication area of the person has been placed on the identification area 2 of the sensor 1 in each case.

Figure 2 is intended to be used to illustrate the ratio of the person's total authentication area to the part of the authentication area which is stored in the memory 4 and to the part of this authentication area which is detected ~~by means of~~ via the identification area of the sensor 1. For the purposes of illustration, the identification of a person by means of the biometric features of a fingerprint is again used as an example. In this case, the authentication area AF is the fingerprint area of a finger of the person. The total range of this authentication area contains biometric features which uniquely identify a person. Of these, the part which is shown shaded is stored in the memory 4. This part is given by the area of the region A less the area of the region B plus a tolerance region ΔA for the region A.

When the person places his finger to be used for identification onto the identification area 2 of the sensor 1, the sensor 1 detects a particular part of the total fingerprint area AF. This is illustrated in Figure 2 ~~by means of~~ via the ellipse surrounding the area A within the region AF. Depending on the position of the finger on the identification area 2 of the sensor 1, this ellipse moves within the region AF stored in the memory 4.

The part of the authentication area which is detected ~~by means of~~ via the sensor 1 is subdivided into two regions A and B. The biometric features of the region A ~~can~~ now can be compared with biometric features of the area AF stored in the memory 4 which have a geometrically identical arrangement. If a match has been determined, the position of the region A within the authentication area AF is obtained unambiguously, and hence so too is the position of the second region B, since the latter region is in a particular, in this case geometrical, relationship with

respect to the region A. This information and the biometric features of the second region B ~~can~~ then can be used to calculate the identification code or the PIN.

Although the present invention has been described with reference to specific embodiments, those of skill in the art will recognize that changes may be made thereto without departing from the spirit and scope of the invention as set forth in the hereafter appended claims.

ABSTRACT OF THE DISCLOSURE

~~Apparatus and method for the biometric identification of a person~~

~~The present invention relates to an~~ An apparatus and ~~to a~~ method for the biometric identification of a person, who has an authentication area ~~(AF)~~ containing biometric features~~.~~, ~~The apparatus comprises~~ the apparatus including a sensor ~~(1)~~ having an identification area ~~(2)~~ for detecting the biometric features of the part of the person's authentication area ~~(AF)~~ which is situated on the identification area ~~(2)~~, a comparison device ~~(5)~~ for comparing the detected biometric features with the biometric features, stored in a memory ~~(4)~~, of a part of the authentication area ~~(AF)~~ of an authorized person or of a ~~plurality~~ number of authorized persons in order to determine the relative position of the biometric features detected by the sensor ~~(1)~~ within the part of the authentication area ~~(AF)~~, and a computation device ~~(5)~~ for calculating an identification code ~~(PIN)~~, which identifies the person detected by the sensor ~~(1)~~, from the detected biometric features which are not stored in the memory ~~(4)~~ on the basis of the relative position of the biometric features which are stored in the memory ~~(4)~~ within the stored authentication area ~~(AF)~~.

Description

Apparatus and method for the biometric identification of a person

The present invention relates to an apparatus and to a method for the biometric identification of a person, who has an authentication area containing biometric features. Such apparatuses and methods are used, for example, in electronic appliances where a user needs to authenticate himself before using the appliance. Examples of such electronic appliances are telecommunication appliances, such as mobile telephones, and computers. In mobile telephones, for example, it is usual to use a so-called personal identification number (PIN) as access authorization. In this context, in order to be able to make a telephone call, the user needs to enter a particular PIN which is known only to him. The mobile telephone checks this PIN and, if the check is positive, enables the mobile telephone for the purpose of making calls.

In addition, more general identification codes, like PINs, are used in computers in order to control access to particular data or services of the computer or of a communication network to which the computer is connected.

Usually, the authentication information is entered using a keypad associated with the apparatus and is then checked. In this way, the authorization of the user making the entry is established by the mobile telephone, the computer or the communication network.

In mobile telephones based on the GSM standard, this is done by virtue of a data processing device on the appliance's 'SIM' card checking whether the entered PIN matches the information stored on the SIM card. If this is the case, the SIM card enables the telephone for use. According to the GSM standard, a particularly high level of security is obtained

for the telephone customer by virtue of the fact that the PIN must not be stored in the mobile telephone itself, but rather is stored on the SIM card in encrypted form only.

In addition, biometric identification methods have recently been developed in which biological or biometric features of a user are used for authentication purposes. By way of example, the fingerprint of a user is used as unique identification of this user. Such biometric identification is a complex but convenient and often very secure method of ensuring that a particular person is associated with and can access a service, an object or a place. In this context, the advantage of biometric identification over the PIN is that it cannot be forgotten, and that the biometric features can be copied only with very great difficulty, or cannot be copied at all. Whereas the PIN is pure software, biometric features always have a more or less unique association with the hardware, i.e. with the body of the authorized user. Since the PIN entails the entry of digits or text, which usually requires a series of keystrokes, this always results in convenience being diminished, and hence sometimes in the security measures being bypassed. For example, with some mobile radio services, the user is able to turn off the PIN completely, at his own risk. Mobile radio services do not require acknowledgement of each individual telephone call by means of the PIN. This means that, once it has been turned on, a mobile telephone can be used by any third parties and hence also by unauthorized persons at the cost of the owner of the mobile telephone. Modern mobile telephones are increasingly trying to restrict the entry of digits for telephone numbers to emergencies. Attempts are even being made to manage with mobile telephones with no keypad at all for some applications. In this case, distinctive biometric identification, if it is possible with little effort, is very advantageous.

In current mobile telephones, however, the problem arises that they require the PIN to be stored on the SIM card in order to conform to standard on the basis of the GSM standard, as explained above. In accordance with the GSM standard, this PIN must not be additionally stored in the mobile telephone itself. The problem which this poses is that the PIN cannot be completely replaced by biometric identification without changing the GSM standard.

For this reason, a method has been proposed in which a unique identification number can be derived from biometric features. This unique identification number can accordingly be used as a PIN and, by way of example, can be forwarded to the SIM card of a mobile telephone. It is evident that, in this case, the PIN is not stored in the mobile telephone itself, but rather is merely calculated by the latter from detected biometric features.

If an authentication area of a person, such as the fingerprint of the person, is used, this authentication area contains biometric features which uniquely identify the person. In this context, the total authentication area, i.e. the fingerprint area, which can be used to identify the user is usually larger than the identification area of a sensor detecting the biometric features of the person's authentication area. This means that the sensor uses only part of the person's authentication area to derive the unique identification number. Accordingly, variations in position, for example of the fingerprint area, on the identification area of the sensor can result in different identification numbers. Such different identification numbers for a user cannot be used as a PIN and make unique identification of the user more difficult.

It is the object of the present invention to provide an apparatus and a method for the biometric identification of a person, who has an authentication area containing biometric features, in which a unique identification number can be derived irrespective of variations in the positioning of the part of the person's authentication area which is situated on the identification area of the sensor.

The invention provides an apparatus for the biometric identification of a person, who has an authentication area containing biometric features, comprising a sensor having an identification area for detecting the biometric features of the part of the person's authentication area which is situated on the identification area, a comparison device for comparing the detected biometric features of the first area with the biometric features, stored in a memory, of a part of the authentication area of an authorized person or of a plurality of authorized persons and for determining the relative position of the biometric features detected by the sensor within the part of the authentication area, and a computation device for calculating an identification code, which identifies the person detected by the sensor, from the detected biometric features which are not stored in the memory 4 on the basis of the relative position of the biometric features which are stored in the memory (4) within the stored authentication area.

An advantage of the apparatus according to the invention is that the identification area of the sensor is split into two regions, with one region being used for position determination within the authentication area while the second region is used to generate a unique identification number, the biometric features of this region not being stored in the apparatus. This ensures that, even if different portions of the user's authentication area are in contact with the

identification area of the sensor, it is always possible to calculate a unique identification code which characterizes the user.

In one embodiment of the invention, the sensor detects the fingerprint of a person, the person's authentication area comprising the possible fingerprint areas of a finger of this person which are not used to calculate the identification code.

The advantage of the use of a fingerprint sensor is that the user can firstly place a finger on the sensor without any particular trouble, and, secondly, the biometric features of the fingerprint area permit particularly reliable identification of the user.

In addition, the present invention provides an appropriate method for the biometric identification of a person by means of an authentication area containing biometric features.

The fact that, in one embodiment of the method, the identification area is subdivided such that the region used for the position determination within the authentication area completely surrounds the area used to calculate the identification code ensures that the second, enclosed region always contains sufficient biometric features to calculate a unique identification code.

Illustrative embodiments of the present invention are now explained with the aid of the drawings.

Figure 1 shows an illustrative embodiment of the present invention, and

Figure 2 shows one possible position of that region of a person's authentication area which is detected by the identification area of the sensor.

In the illustrative embodiment explained here, the present invention is explained using an apparatus and a method which uses a person's fingerprint to identify this person. Hence, the person's authentication area is part of the total fingerprint area of a finger of this person. In addition, the biometric features of the fingerprint area are the line ends and bifurcations of the corresponding fingerprint.

Figure 1 shows, schematically, an illustrative embodiment of the apparatus according to the invention. The sensor 1 is used to detect part of the total fingerprint area of a finger of the person who is to be identified. To this end, the sensor 1 has an identification area 2 onto which the user places the finger. Since the identification area 2 is smaller than the total fingerprint area of a finger, the identification area 2 is used to detect a particular portion of the fingerprint. The identification area 2 is used to detect the biometric features of the part of the total fingerprint area which is in contact. The information detected by the sensor 1 is supplied to a comparison device 5.

When the apparatus is initialized, i.e. before a person is first identified, the part of the total authentication area of the authorized person(s) which is required to determine the position of the detected biometric features is stored in a memory 4. By way of example, a region of the area A - B $+\Delta A$ may be stored, where ΔA forms a ring having a particular tolerance width around A. In the illustrative embodiment described in this case, this means that the fingerprint area of a finger of the

authorized person(s) which is used to determine the identification code is not stored in the memory 4.

The comparison device 5, which is connected both to the sensor 1 and to the memory 4, compares the detected biometric features with the biometric features stored in the memory 4. A match between the biometric features of a region A, for example, and a geometric region within the authentication area stored in the memory 4 gives the relative position of the detected region A within the authentication area. This comparison gives the information about which part of the fingerprint has been placed onto the identification area 2 of the sensor 1. Hence, the outer region A is used for centering, while the central region B surrounded by the region A is used later to generate the identification code or the PIN. The regions A, B are thus advantageously chosen such that the outer region A forms a ring, containing biometric features, which completely surrounds the central region B. However, in another embodiment of the invention, the biometric features may also be split into two regions differently. By way of example, the right-hand and left-hand halves or the top and bottom halves could be chosen as the subdivision. In addition, the branches and the line ends of the fingerprint could be used as the subdivision.

For the purposes of centering, it is not absolutely necessary for the outer region A to be complete, i.e. to contain biometric features throughout. If there are variations in the contact of the finger on the identification area 2, it is possible that no biometric features are detected at the extreme edge of the outer region A. If, however, biometric features are detected in a closed ring, surrounding the central region B, of the outer region A and have their position determined by means of comparison with the authentication area stored in the memory 4, then at least the central region B is

available in its entirety and in the correct position. In addition, in a learning phase when the apparatus is initialized, it is possible for an algorithm to decide what belongs to the central region B and what belongs to the outer region A.

The comparison device 5 supplies the result of the position determination for the part of the total fingerprint area which is detected by the sensor 1 to a computation device 6. The computation device 6 calculates from the biometric features of the central region B, whose relative position is determined from the position of the region A, an identification code which uniquely identifies the person detected by the sensor 1. This identification code may be a PIN, for example, which is supplied to the SIM card of the mobile telephone.

Hence, neither the PIN nor the biometric features from which the PIN is calculated is/are stored in the inventive apparatus itself. The only thing stored in the memory 4 of the apparatus is part of the authentication area containing biometric features. The sensor 1 is used to detect biometric features of a person, and the computation device 6 is used to convert them into a PIN which can then be output. In addition, the person's PIN or identification code can be derived even if, for different identification operations, a different part of the authentication area of the person has been placed on the identification area 2 of the sensor 1 in each case.

Figure 2 is intended to be used to illustrate the ratio of the person's total authentication area to the part of the authentication area which is stored in the memory 4 and to the part of this authentication area which is detected by means of the identification area of the sensor 1. For the purposes of illustration, the identification of a person by means of the biometric features of a fingerprint is again used as an example. In this case, the authentication area AF is the

fingerprint area of a finger of the person. The total

range of this authentication area contains biometric features which uniquely identify a person. Of these, the part which is shown shaded is stored in the memory 4. This part is given by the area of the region A less the area of the region B plus a tolerance region ΔA for the region A.

When the person places his finger to be used for identification onto the identification area 2 of the sensor 1, the sensor 1 detects a particular part of the total fingerprint area AF. This is illustrated in Figure 2 by means of the ellipse surrounding the area A within the region AF. Depending on the position of the finger on the identification area 2 of the sensor 1, this ellipse moves within the region AF stored in the memory 4.

The part of the authentication area which is detected by means of the sensor 1 is subdivided into two regions A and B. The biometric features of the region A can now be compared with biometric features of the area AF stored in the memory 4 which have a geometrically identical arrangement. If a match has been determined, the position of the region A within the authentication area AF is obtained unambiguously, and hence so too is the position of the second region B, since the latter region is in a particular, in this case geometrical, relationship with respect to the region A. This information and the biometric features of the second region B can then be used to calculate the identification code or the PIN.

Patent Claims

1. An apparatus for the biometric identification of a person, who has an authentication area (AF) containing biometric features, comprising:

- a sensor (1) having an identification area (2) for detecting the biometric features of the part of the person's authentication area (AF) which is situated on the identification area (2),
- a comparison device (5) for comparing the detected biometric features with the biometric features, stored in a memory (4), of a part of the authentication area (AF) of an authorized person or of a plurality of authorized persons in order to determine the relative position of the biometric features, detected by the sensor (1), of the first detected region (A) within the part of the authentication area (AF), and
- a computation device (5) for calculating an identification code (PIN), which identifies the person detected by the sensor (1), from the detected biometric features which are not stored in the memory (4) on the basis of the relative position of the biometric features which are stored in the memory (4) within the stored authentication area (AF).

2. The apparatus as claimed in claim 1, characterized in that the sensor (1) detects a fingerprint, the authentication area comprising those parts of the possible fingerprint area of a finger which are not used to calculate the identification code (PIN).

3. A method for the biometric identification of a person, who has an authentication area (AF) containing biometric features, comprising the following steps:

- biometric features of a part of the authentication area (AF) of an authorized person or of a plurality of authorized persons are stored,
- biometric features of the part of the person's authentication area (AF) which is situated on the identification area (2) are detected,
- the detected biometric features are compared with the stored biometric features of the authentication area (AF) in order to determine the relative position of the detected biometric features within the stored part of the authentication area (AF),
- an identification code (PIN) which identifies the person detected by the sensor (1) is calculated from the detected biometric features which are not stored in the memory (4) on the basis of the relative position of the biometric features which are stored in the memory 4 within the stored authentication area (AF).

4. The method as claimed in claim 3, characterized in that biometric features of a person's fingerprint are detected, and the authentication area (AF) comprises those parts of the possible fingerprint areas of a finger of the person which are not used to calculate the identification code (PIN).

5. The method as claimed in claim 3 or 4, characterized in that a first region (A) containing biometric features which are stored in the memory (4) completely surrounds a second region (B) containing biometric features which are not stored in the memory (4).

6. The method as claimed in one of claims 3 to 5,

characterized
in that an identification code (PIN) is calculated only if the detected first region (A) forms a closed ring, surrounding the second region (B), containing biometric features.

GR 98 P 2902

Abstract

Apparatus and method for the biometric identification of a person

The present invention relates to an apparatus and to a method for the biometric identification of a person, who has an authentication area (AF) containing biometric features. The apparatus comprises a sensor (1) having an identification area (2) for detecting the biometric features of the part of the person's authentication area (AF) which is situated on the identification area (2), a comparison device (5) for comparing the detected biometric features with the biometric features, stored in a memory (4), of a part of the authentication area (AF) of an authorized person or of a plurality of authorized persons in order to determine the relative position of the biometric features detected by the sensor (1) within the part of the authentication area (AF), and a computation device (5) for calculating an identification code (PIN), which identifies the person detected by the sensor (1), from the detected biometric features which are not stored in the memory (4) on the basis of the relative position of the biometric features which are stored in the memory (4) within the stored authentication area (AF).

(Figure 1)

Declaration and Power of Attorney For Patent Application
Erklärung Für Patentanmeldungen Mit Vollmacht
German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Vorrichtung und Verfahren zur biometrischen Identifikation einer Person

Device and method for identifying a person by biometric characteristics

deren Beschreibung

the specification of which

(zutreffendes ankreuzen)
☐ hier beigefügt ist.
☒ am 17.08.1999 als
PCT internationale Anmeldung
PCT Anmeldungsnummer PCT/DE99/02572
eingereicht wurde und am _____
abgeändert wurde (falls tatsächlich abgeändert).

(check one)
☐ is attached hereto.
☒ was filed on 17.08.1999 as
PCT international application
PCT Application No. PCT/DE99/02572
and was amended on _____
(if applicable)

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign appplications
Priorität beansprucht

			Priority Claimed	
19847415.6	DE	14.10.1998	☒	☐
(Number)	(Country)	(Day Month Year Filed)	Yes	No
(Nummer)	(Land)	(Tag Monat Jahr eingereicht)	Ja	Nein
			☐	☐
(Number)	(Country)	(Day Month Year Filed)	Yes	No
(Nummer)	(Land)	(Tag Monat Jahr eingereicht)	Ja	Nein
			☐	☐
(Number)	(Country)	(Day Month Year Filed)	Yes	No
(Nummer)	(Land)	(Tag Monat Jahr eingereicht)	Ja	Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

PCT/DE99/02572	17.08.1999		
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date D, M, Y) (Anmeldedatum T, M, J)	(Status) (patentiert, anhangig, aufgegeben)	(Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date D,M,Y) (Anmeldedatum T, M; J)	(Status) (patentiert, anhangig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Customer No.

And I hereby appoint

Telefongespräche bitte richten an: *(Name und Telefonnummer)*

Direct Telephone Calls to: *(name and telephone number)*

Ext. _____

Postanschrift:

Send Correspondence to:

Bell, Boyd & Lloyd LLC
70 West Madison Street, Suite 3300 60602-4207 Chicago, Illinois
Telephone: +1 312 372 1121 and Facsimile +1 312 372 2098
or
Customer No.

Voller Name des einzigen oder ursprünglichen Erfinders:	Full name of sole or first inventor:
Dr. MANFRED BROMBA	Dr. MANFRED BROMBA
Unterschrift des Erfinders Datum: Manfred Bromba 01.03.13	Inventor's signature Date
Wohnsitz: MUENCHEN, DEUTSCHLAND DEX	Residence: MUENCHEN, GERMANY
Staatsangehorigkeit: DE	Citizenship: DE
Postanschrift: AM ISARKANAL 24 81379 MUENCHEN	Post Office Addess: AM ISARKANAL 24 81379 MUENCHEN
Voller Name des zweiten Miterfinders (falls zutreffend): BERNHARD RAAF	Full name of second joint inventor, if any: BERNHARD RAAF
Unterschrift des Erfinders Datum: Bernhard Raaf 6.3.07	Second Inventor's signature Date: Manfred Bromba 01.03.13
Wohnsitz: MUENCHEN, DEUTSCHLAND	Residence: MUENCHEN, GERMANY
Staatsangehorigkeit: DE DEX	Citizenship: DE
Postanschrift: MAXHOFSTR. 62 81475 MUENCHEN	Post Office Address: MAXHOFSTR. 62 81475 MUENCHEN

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).